3-2010

Location of quantum information in additive graph codes

Vlad Gheorghiu
Carnegie Mellon University

Shiang Yong Looi
Carnegie Mellon University, phylsy@cmu.edu

Robert B. Griffiths
Carnegie Mellon University, rgrif@cmu.edu

Published In
Phys. Rev. A, 81, 032326.

Location of quantum information in additive graph codes

Vlad Gheorghiu,* Shiang Yong Looi,† and Robert B. Griffiths
Department of Physics, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, USA
(Received 17 December 2009; published 25 March 2010)

The location of quantum information in various subsets of the qudit carriers of an additive graph code is discussed using a collection of operators on the coding space which form what we call the *information group*. It represents the input information through an encoding operation constructed as an explicit quantum circuit. Partial traces of these operators down to a particular subset of carriers provide an isomorphism of a subgroup of the information group, and this gives a precise characterization of what kinds of information they contain. All carriers are assumed to have the same dimension D, an arbitrary integer greater than 1.

DOI: 10.1103/PhysRevA.81.032326 PACS number(s): 03.67.Pp, 03.67.Mn

I. INTRODUCTION

Quantum codes in which quantum information is redundantly encoded in a collection of code carriers play an important role in quantum information, in particular in systems for error correction and in schemes for quantum communication [1–4]. They are a generalization of the classical codes well known and widely used in everyday communication systems [5]. While for the latter it is fairly obvious where the information is located, the quantum case is more complicated for two reasons. First, a quantum Hilbert space with its noncommuting operators is a more complex mathematical structure than the strings of bits or other integers used in classical codes. Second, the very concept of "information" is not easy to define in the quantum case. However, in certain cases one is able to make quite precise statements. Thus in the five qubit code [6] that encodes one qubit of information, none of the encoded information is present in any two qubits taken by themselves, whereas all the information can be recovered from any set of three qubits [7].

Similar precise statements can be made, as we shall see, in the case of an *additive graph code* on a collection of n qudits which constitute the *carriers* of the code, provided each qudit has the same dimension D, with D some integer greater than one (not necessarily prime). It was shown in [8] that all additive graph codes are stabilizer codes, and in [9,10] that all stabilizer codes are equivalent to graph codes for prime D. A detailed discussion of nonbinary quantum error correcting codes can be found in [8,11–14]. The five qubit code just mentioned is an example of a quantum code that is locally equivalent to an additive graph code [13], and the information location has an "all or nothing" character. In general the situation is more interesting in that some subset of carriers may contain some but not all of the encoded information, and what is present can be either "classical" or "quantum," or a mixture of the two. Since many of the best codes currently known are additive graph codes, identifying the location of information could prove useful when utilizing codes for error correction, or designing new or better codes, or codes that correct some types of errors more efficiently than others [15]. Our formalism can also be applied to study quantum secret sharing schemes employing graph states and can even handle a more general setting where there might be subsets that contain partial information and hence are neither authorized (contain the whole quantum secret) nor unauthorized (contain no information whatsoever about the secret).

Our approach to the problem of information location is algebraic, based upon the fact that generalized Pauli operators on the Hilbert space of the carriers form a group. Subgroups of this group can be associated with different types of information, and the information available in some subset of the carriers can also be identified with, or is isomorphic to, an appropriate subgroup, as indicated in the isomorphism theorem of Sec. V. In the process of deriving this theorem we go through a series of steps which amount to an *encoding procedure* that takes the initial quantum information and places it in the coding subspace of the carrier Hilbert space. These steps can in turn be transformed into a set of quantum gates to produce an explicit circuit that carries out the encoding. This result, although somewhat subsidiary to our main aims, is itself not without interest, and is an alternative to a previous scheme [13] limited to prime D.

There have been some previous studies of quantum channels using an algebraic approach similar to that employed here. Those most closely related to our work are by Bény *et al.* [16,17] (and see Bény [18]) and Blume-Kohout *et al.* [19]. These authors have provided a set of very general conditions under which an algebraic structure is preserved by a channel. In Appendix D we show that our results fit within the framework of a "correctable algebra" as defined in [16–18]. See also the remarks in Sec. VII.

The remainder of this paper is organized as follows. Some general comments about types of quantum information and their connection with certain ideal quantum channels are found in Sec. II. Section III contains definitions of the Pauli group and of some quantum gates used later in the paper. The formalism associated with additive graph codes as well as our encoding strategy is in Sec. IV; this along with some results on partial traces leads to the fundamental isomorphism result in Sec. V, which also indicates some of its consequences for the types of information discussed in Sec. II. Section VI contains various applications to specific codes, for both qubit and qudit carriers. Finally, Sec. VII contains a summary, conclusions, and some open questions. Appendices A and B contain longer proofs

*vgheorgh@andrew.cmu.edu
†slooi@andrew.cmu.edu

of theorems, Appendix C presents an efficient linear algebra based algorithm for working out the results for any additive graph code, and Appendix D illustrates the connection with related work in [16] and [17].

II. TYPES OF INFORMATION

Both classical and quantum information theory have to do with statistical correlations between properties of two or more systems, or properties of a single system at two or more times. In the classical case information is always related to a possible set of physical properties that are distinct and mutually exclusive—e.g., the voltage has one of a certain number of values—with one and only one of these properties realized in a particular system at a particular time. For quantum systems it is useful to distinguish different *types* or *species* of information [20], each corresponding to a collection of mutually distinct properties represented by a (projective) decomposition $\mathcal{J} = \{J_j\}$ of the identity I on the relevant Hilbert space $\mathcal{H}$:

$$I = \sum_j J_j, \quad J_j = J_j^\dagger = J_j^2, \quad J_j J_k = \delta_{jk} J_j. \tag{1}$$

Any normal operator M has a spectral representation of the form

$$M = \sum_j \mu_j J_j, \tag{2}$$

where the μ_j are its eigenvalues, and the decomposition $\{J_j\}$ is uniquely specified by requiring $\mu_j \neq \mu_k$ when $j \neq k$. This means one can sensibly speak about the type of information $\mathcal{J}(M)$ *associated with* a normal operator M. When M is Hermitian this is the kind of information obtained by measuring M.

This terminology allows one to discuss the transmission of information through a quantum channel in the following way. Let $\mathcal{E}$ be the completely positive, trace preserving superoperator that maps the space of operators $\mathcal{L}(\mathcal{H})$ of the channel input onto the corresponding operator space $\mathcal{L}(\mathcal{H}')$ of the channel output $\mathcal{H}'$ (which may have a different dimension from $\mathcal{H}$). Provided

$$\mathcal{E}(J_j)\mathcal{E}(J_k) = 0 \quad \text{for} \quad j \neq k, \tag{3}$$

for all the operators $\{J_j\}$ associated with a decomposition $\mathcal{J}$ of the $\mathcal{H}$ identity, we shall say the channel is *ideal* or *noiseless* for the $\mathcal{J}$ species of information, or, equivalently, the $\mathcal{J}$ type of information is *perfectly present* in the channel output $\mathcal{H}'$. Formally, each physical property J_j at the input corresponds in a one-to-one fashion to a unique property, the support of $\mathcal{E}(J_j)$ (or the corresponding projector) at the output. Thus we have a quantum version of a noiseless classical channel, a device for transmitting symbols, in this case the label j on J_j, from the input to the output by associating distinct symbols with distinct physical properties—possibly a different collection of properties at the output than at the input.

The opposite extreme from a noiseless channel is one in which $\mathcal{E}(J_j)$ is *independent of* j up to a multiplicative constant. In this case no information of type $\mathcal{J}$ is available at the channel output: the channel is *blocked*, or completely noisy; equivalently, the $\mathcal{J}$ species of information is *absent* from the channel output. Hereafter we shall always use "absent" in the strong sense of "completely absent" and the term *present*, or *partially present* for situations in which some type of information is not (completely) absent but is also not perfectly present: i.e., the channel is noisy but not completely blocked for this type of information.

In some cases all the projectors in $\{J_j\}$ will be of rank 1, onto pure states, but in other cases some or all of them may be of higher rank, in which case one may have a *refinement* $\mathcal{L} = \{L_l\}$ of $\{J_j\}$ such that each projector J_j is a sum of one or more projectors from the $\mathcal{L}$ decomposition. It is then clear that if the $\mathcal{L}$ information is absent from (perfectly present in) the channel output the same is true of the $\mathcal{J}$ information, but the converse need not hold. Thus it may be that the coarse grained $\mathcal{J}$ information is perfectly present, but no additional information is available about the refinement. A particularly simple situation, which we will encounter later, is one in which the output $\mathcal{H}'$ is itself a tensor product, say $\mathcal{H}'_1 \otimes \mathcal{H}'_2$, $\mathcal{J}$ a decomposition of $\mathcal{H}'_1$, $\mathcal{J} = \{J_j \otimes I\}$ and $\mathcal{K}$ a decomposition of $\mathcal{H}'_2$, $\mathcal{K} = \{I \otimes K_k\}$. It can then be the case that the information associated with the $\mathcal{J}$ decomposition is perfectly present and that associated with the $\mathcal{K}$ decomposition is (perfectly) absent from the channel output.

Suppose $\mathcal{J} = \{J_j\}$ and $\mathcal{K} = \{K_k\}$ are two types of quantum information defined on the same Hilbert space. The species $\mathcal{J}$ and $\mathcal{K}$ are *compatible* if all the projectors in $\mathcal{J}$ commute with all the projectors in $\mathcal{K}$, in which case the distinct nonzero projectors in the collection $\{J_j K_k\}$ provide a common refinement of the type discussed above. Otherwise, if some projectors in one collection do not commute with certain projectors in the other, $\mathcal{J}$ and $\mathcal{K}$ are *incompatible* and cannot be combined with each other. This is an example of the single framework rule of consistent quantum reasoning (see [21] or Chap. 16 of [22]). The same channel may be ideal for some $\mathcal{J}$ and blocked for some $\mathcal{K}$, or noisy for both but with different amounts of noise. From a quantum perspective, classical information theory is only concerned with a single type of (quantum) information, or several compatible types which possess a common refinement, whereas the task of quantum, in contrast to classical, information theory is to analyze situations where multiple incompatible types need to be considered.

The term "classical information" when used in a quantum context can be ambiguous or misleading. Generally it is used when only a single type of information, corresponding to a single decomposition of the identity, suffices to describe what emerges from a channel, and other incompatible types can therefore be ignored. Even in such cases it is helpful to indicate explicitly which decomposition of the identity is involved if that is not obvious from the context. The contrasting term "quantum information" can then refer to situations where two or more types of information corresponding to incompatible decompositions are involved, and again it is helpful to be explicit about what one has in mind if there is any danger of ambiguity.

An *ideal quantum channel* is one in which there is an isometry V from $\mathcal{H}$ to $\mathcal{H}'$ such that

$$\mathcal{E}(A) = VAV^\dagger \tag{4}$$

for every operator A on $\mathcal{H}$. In this case the superoperator $\mathcal{E}$ preserves not only sums but also operator products:

$$\mathcal{E}(AB) = \mathcal{E}(A)\mathcal{E}(B). \tag{5}$$

Conversely, if (5) holds for any pair of operators, one can show that the quantum channel is ideal [16,17], i.e., $\mathcal{E}$ has the form (4). As the isometry maps orthogonal projectors to orthogonal projectors, (3) will be satisfied for every species of information, and we shall say that *all* information is perfectly present at the channel output. The converse, that a channel which is ideal for all species, or even for an appropriately chosen pair of incompatible species is an ideal quantum channel, is also correct; see [7,20].

The preservation of operator products, (4), can be a very useful tool in checking for the presence or absence of various types of information in the channel output, as we shall see in Sec. V. When (5) holds for arbitrary A and B belonging to a particular decomposition of the identity, this suffices to show that the channel is ideal for this species. However, note that this sufficient condition is not necessary, since (3) could hold without the $\mathcal{E}(A_j)$ being projectors, in which case $\mathcal{E}(A_j^2)$ is not mapped to $\mathcal{E}(A_j)^2$.

We use the term *ideal classical channel* for a type of information $\mathcal{J} = \{J_j\}$ to refer to a situation where (3) is satisfied and, in addition,

$$\mathcal{E}(J_j A J_k) = 0 \quad \text{for} \quad j \neq k, \tag{6}$$

where A is any operator on the input Hilbert space $\mathcal{H}$. That is, not only is type $\mathcal{J}$ perfectly transmitted, but all other types are "truncated" relative to this type, in the notation of [21].

III. PRELIMINARY REMARKS AND DEFINITIONS

A. Generalized Pauli operators on *n* qudits

We generalize Pauli operators to higher dimensional systems of arbitrary dimension D in the following way. The X and Z operators acting on a single qudit are defined as

$$Z = \sum_{j=0}^{D-1} \omega^j |j\rangle\langle j|, \quad X = \sum_{j=0}^{D-1} |j\rangle\langle j+1| \tag{7}$$

and satisfy

$$X^D = Z^D = I, \quad XZ = \omega ZX, \quad \omega = e^{2\pi \mathrm{i}/D}, \tag{8}$$

where *the addition of integers is modulo* D, as will be assumed from now on. For a collection of n qudits we use subscripts to identify the corresponding Pauli operators: thus Z_i and X_i operate on the space of qudit i. The Hilbert space of a single qudit is denoted by $\mathcal{H}$, and the Hilbert space of n qudits by $\mathcal{H}_n$, respectively. Operators of the form

$$\omega^\lambda X^{\mathbf{x}} Z^{\mathbf{z}} := \omega^\lambda X_1^{x_1} Z_1^{z_1} \otimes X_2^{x_2} Z_2^{z_2} \otimes \cdots \otimes X_n^{x_n} Z_n^{z_n} \tag{9}$$

will be referred to as *Pauli products*, where λ is an integer in $\mathbb{Z}_D$ and $\mathbf{x}$ and $\mathbf{z}$ are n-tuples in $\mathbb{Z}_D^n$, the additive group of n-tuple integers mod D. For a fixed n the collection of all possible Pauli products (9) form a group under operator multiplication, the *Pauli group* $\mathcal{P}_n$. If p is a Pauli product, then $p^D = I$ is the identity operator on $\mathcal{H}_n$, and hence the order of any element of $\mathcal{P}_n$ is either D or else an integer that divides D. While $\mathcal{P}_n$ is not Abelian, it has the property that two elements *commute up to a phase*: $p_1 p_2 = \omega^{\lambda_{12}} p_2 p_1$, with λ_{12} an integer in $\mathbb{Z}_D$ that depends on p_1 and p_2.

The collection of Pauli products with $\lambda = 0$, i.e., a prefactor of 1, is denoted by $\mathcal{Q}_n$ and forms an orthonormal basis of $\mathcal{L}(\mathcal{H}_n)$, the Hilbert space of linear operators on $\mathcal{H}_n$, with respect to the inner product

$$\frac{1}{D^n} \mathrm{Tr}[q_1^\dagger q_2] = \delta_{q_1,q_2}, \quad \forall q_1, q_2 \in \mathcal{Q}_n. \tag{10}$$

Note that $\mathcal{Q}_n$ is a *projective group* or group up to phases. There is a bijective map between $\mathcal{Q}_n$ and the quotient group $\mathcal{P}_n/\{\omega^\lambda I\}$ for $\lambda \in \mathbb{Z}_D$ where $\{\omega^\lambda I\}$, the center of $\mathcal{P}_n$, consists of phases multiplying the identity operator on n qudits.

B. Generalization of qubit quantum gates to higher dimensions

In this subsection we define some one and two qudit gates generalizing various qubit gates. The qudit generalization of the Hadamard gate is the *Fourier gate*

$$\mathrm{F} := \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} \omega^{jk} |j\rangle\langle k|. \tag{11}$$

For an invertible integer $q \in \mathbb{Z}_D$ (i.e., an integer for which there exists $\bar{q} \in \mathbb{Z}_D$ such that $q\bar{q} \equiv 1 \bmod D$), we define a *multiplicative gate*

$$\mathrm{S}_q := \sum_{j=0}^{D-1} |j\rangle\langle jq|, \tag{12}$$

where qj means multiplication mod D. The requirement that q be invertible ensures that S_q is unitary; for a qubit S_q is just the identity.

For two distinct qudits a and b we define the controlled-NOT (CNOT) gate as

$$\mathrm{CNOT}_{ab} := \sum_{j=0}^{D-1} |j\rangle\langle j|_a \otimes X_b^j = \sum_{j,k=0}^{D-1} |j\rangle\langle j|_a \otimes |k\rangle\langle k+j|_b, \tag{13}$$

the obvious generalization of the qubit controlled-NOT, where a labels the control qudit and b labels the target qudit. Next the SWAP gate is defined as

$$\mathrm{SWAP}_{ab} := \sum_{j,k=0}^{D-1} |k\rangle\langle j|_a \otimes |j\rangle\langle k|_b. \tag{14}$$

It is easy to check that the SWAP gate is Hermitian and does indeed swap qudits a and b. Unlike the qubit case, the qudit SWAP gate is not a product of three CNOT gates but can be expressed in terms of CNOT gates and Fourier gates as

$$\mathrm{SWAP}_{ab} = \mathrm{CNOT}_{ab}(\mathrm{CNOT}_{ba})^\dagger \mathrm{CNOT}_{ab}\left(\mathrm{F}_a^2 \otimes I_b\right), \tag{15}$$

with

$$(\mathrm{CNOT}_{ba})^\dagger = (\mathrm{CNOT}_{ba})^{D-1} = \left(I_a \otimes \mathrm{F}_b^2\right)\mathrm{CNOT}_{ba}\left(I_a \otimes \mathrm{F}_b^2\right). \tag{16}$$

TABLE I. The conjugation of Pauli operators by one-qudit gates F and S_q (where $\bar{q}$ is the multiplicative inverse of q mod D).

Pauli operator	S_q	F
Z	Z^q	X
X	$X^{\bar{q}}$	Z^{D-1}

Finally we define the generalized controlled-phase or CP gate as

$$\mathrm{CP}_{ab} = \sum_{j=0}^{D-1} |j\rangle\langle j|_a \otimes Z_b^j = \sum_{j,k=0}^{D-1} \omega^{jk} |j\rangle\langle j|_a \otimes |k\rangle\langle k|_b. \tag{17}$$

The CP and CNOT gates are related by a local Fourier gate, similar to the qubit case:

$$\mathrm{CNOT}_{ab} = (I_a \otimes \mathrm{F}_b)\mathrm{CP}_{ab}(I_a \otimes \mathrm{F}_b)^\dagger, \tag{18}$$

since F maps Z into X under conjugation (see Table I).

The gates F, S_q, SWAP, CNOT, and CP are unitary operators that map Pauli operators to Pauli operators under conjugation, as can be seen from Tables I and II. They are elements of the so called *Clifford group* on n qudits [11,23], the group of n-qudit unitary operators that leaves $\mathcal{P}_n$ invariant under conjugation, i.e. if O is a Clifford operator, then $\forall p \in \mathcal{P}_n$, $OpO^\dagger \in \mathcal{P}_n$. From Tables I and II one can easily deduce the result of conjugation by F, S_q, SWAP, CNOT, and CP on *any* Pauli product.

IV. GRAPH STATES, GRAPH CODES, AND RELATED OPERATOR GROUPS

A. Graph states and graph codes

Let $G = (V, E)$ be a graph with n vertices V, each corresponding to a qudit, and a collection E of undirected edges connecting pairs of distinct vertices (no self-loops). Two qudits can be joined by multiple edges, as long as the multiplicity does not exceed $D-1$. The graph G is completely specified by the *adjacency matrix* Γ, where the matrix element Γ_{ab} represents the number of edges that connect vertex a with vertex b. The *graph state*

$$|G\rangle = U|G_0\rangle = U(|+\rangle^{\otimes n}) \tag{19}$$

is obtained by applying the unitary (Clifford) operator

$$U = \prod_{(a,b)\in E} (\mathrm{CP}_{ab})^{\Gamma_{ab}}, \tag{20}$$

TABLE II. The conjugation of Pauli products on qudits a and b by two-qudit gates CNOT, SWAP, and CP. For the CNOT gate, the first qudit a is the control and the second qudit b is the target.

Pauli product	CNOT_{ab}	SWAP_{ab}	CP_{ab}
$I_a \otimes Z_b$	$Z_a \otimes Z_b$	$Z_a \otimes I_b$	$I_a \otimes Z_b$
$Z_a \otimes I_b$	$Z_a \otimes I_b$	$I_a \otimes Z_b$	$Z_a \otimes I_b$
$I_a \otimes X_b$	$I_a \otimes X_b$	$X_a \otimes I_b$	$Z_a^{D-1} \otimes X_b$
$X_a \otimes I_b$	$X_a \otimes X_b^{D-1}$	$I_a \otimes X_b$	$X_a \otimes Z_b^{D-1}$

where each pair (a, b) of vertices occurs only once in the product, to the *trivial graph state*

$$|G_0\rangle := |+\rangle^{\otimes n}, \tag{21}$$

with

$$|+\rangle := \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} |j\rangle. \tag{22}$$

Define $\mathcal{S}^G$ to be the stabilizer of $|G\rangle$, the subgroup of operators from $\mathcal{P}_n$ that leave $|G\rangle$ unchanged. The stabilizer $\mathcal{S}_0^G$ of the trivial graph state $|G_0\rangle$ is simply the set of all X-type Pauli products with no additional phases,

$$\mathcal{S}_0^G = \{X^{\mathbf{x}} : \mathbf{x} = (x_1, x_2, \ldots, x_n)\}, \tag{23}$$

where x_j are arbitrary integers between 0 and $D-1$. Since $|G\rangle$ is related to $|G_0\rangle$ through a Clifford operator [see (19) and (20)], it follows at once that the stabilizer $\mathcal{S}^G$ of $|G\rangle$ is related to the stabilizer $\mathcal{S}_0^G$ of the trivial graph through the Clifford conjugation

$$\mathcal{S}^G = U\mathcal{S}_0^G U^\dagger, \tag{24}$$

with U defined in (20).

A *graph code* C can be defined as the K-dimensional subspace $\mathcal{H}_C$ of $\mathcal{H}_n$ spanned by a collection of K mutually orthogonal codewords

$$|\mathbf{c}_j\rangle = Z^{\mathbf{c}_j}|G\rangle, \quad j = 1, 2, \ldots, K, \tag{25}$$

where

$$\mathbf{c}_j = (c_{j1}, c_{j2}, \ldots, c_{jn}) \tag{26}$$

is for each j an n-tuple in $\mathbb{Z}_D^n$. The c_{jk} notation suggests a matrix $\mathbf{c}$ with K rows and n columns, of integers between 0 and $D-1$, and this is a very helpful perspective. In this paper we are concerned with *additive* graph codes, meaning that the rows of this matrix form a group under component-wise addition mod D, isomorphic to the Abelian *coding group* $\mathcal{C}$, of order $|\mathcal{C}| = K$, of the operators $Z^{\mathbf{c}_j}$ under multiplication. We use $(\mathcal{C}, |G\rangle)$ to denote the corresponding graph code. For more details about graph states and graph codes for arbitrary D, see [8].

Note that the codeword $(0, 0, \ldots, 0)$ is just the graph state $|G\rangle$, and in the case of the trivial graph $|G_0\rangle$ this is the tensor product of $|+\rangle$ states (21), not the tensor product of $|0\rangle$ states which the n-tuple notation $(0, 0, \ldots, 0)$ might suggest. Overlooking this difference can lead to confusion through interchanging the role of X and Z operators, which is the reason for pointing it out here.

B. The encoding problem

A coding group $\mathcal{C}$ can be used to create an additive code starting with any n-qudit graph state, including the trivial graph $|G_0\rangle$, because the entangling unitary U commutes with $Z^{\mathbf{z}}$ for any $\mathbf{z}$; thus

$$|\mathbf{c}_j\rangle = Z^{\mathbf{c}_j}U|G_0\rangle = UZ^{\mathbf{c}_j}|G_0\rangle = U|\mathbf{c}_j^0\rangle, \tag{27}$$

where the $|\mathbf{c}_j^0\rangle$ span the code $(\mathcal{C}, |G_0\rangle)$. But in addition the coding group $\mathcal{C}$ is isomorphic, as explained below, to a *trivial*

code $\mathcal{C}_0$,

$$\mathcal{C}_0 = \langle Z_1^{m_1}, Z_2^{m_2}, \ldots, Z_k^{m_k} \rangle, \tag{28}$$

which is *generated by*, i.e., includes all products of the operators inside the angular brackets $\langle\ \rangle$. Here k is an integer less than or equal to n, and each m_j is 1 or a larger integer that divides D. The simplest situation is the one in which each of the m_j is equal to 1, in which case $\mathcal{C}_0$ is nothing but the group, of order D^k, of products of Z operators to any power less than D on the first k qudits. One can think of these qudits as comprising the input system through which information enters the code, while the remaining $n-k$ qudits, each initially in a $|+\rangle$ state, form the ancillary system for the encoding operation.

If, however, one of the m_j is greater than 1, the corresponding generator $Z_j^{m_j}$ is of order

$$d_j = D/m_j \tag{29}$$

and represents a qudit of dimensionality d_j rather than D. Thus, for example, if $D=6$ and $m_1=2$, applying Z_1^2 and its powers to $|+\rangle$ will produce three orthogonal states corresponding to a qutrit, $d_1=3$. (Identifying operators Z and X on these three states which satisfy (8) with $D=3$ is not altogether trivial and is worked out in Sec. IV C below.) In general one can think of the group $\mathcal{C}_0$ in (28) as associated with a collection of k qudits, the jth qudit having dimension d_j, and therefore the collection as a whole a dimension of $K = d_1 d_2 \cdots d_k$, equal to that of the graph code. If one thinks of the information to be encoded as initially present in these k qudits, the encoding problem is how to map them in an appropriate way into the coding subspace $\mathcal{H}$ of the n (D-dimensional) carriers.

We address this by first considering the connection between $\mathcal{C}$ and $\mathcal{C}_0$ in a simple example with $n=3$, $D=6$, and

$$\mathcal{C} = \langle Z_1^4 Z_2^3 Z_3^3, Z_2^3 Z_3^3 \rangle, \tag{30}$$

a coding group of order 6. The two generators in (30) correspond, in the notation introduced in (26), to the rows of the 2×3 matrix

$$\mathbf{f} = \begin{pmatrix} 4 & 3 & 3 \\ 0 & 3 & 3 \end{pmatrix}. \tag{31}$$

By adding rows or multiplying them by constants mod D one can create four additional rows which together with those in (31) constitute the 6×3 **c** matrix.

Through a sequence of elementary operations mod D—(a) interchanging of rows or columns, (b) multiplication of a row or column by an *invertible* integer, (c) addition of any multiple of a row or column to a *different* row or column—a matrix such as **f** can be converted to the Smith normal form [24,25]

$$\mathbf{s} = \mathbf{v}\cdot\mathbf{f}\cdot\mathbf{w}, \tag{32}$$

where **v** and **w** are invertible (in the mod D sense) square matrices, and **s** is a diagonal rectangular matrix, as in (33). It is proved in [25] that a $K\times n$ matrix can be reduced to the Smith form in only $O(K^{\theta-1}n)$ operations from $\mathbb{Z}_D$, where θ is the exponent for matrix multiplication over the ring $\mathbb{Z}_D$, i.e. two $m\times m$ matrices over $\mathbb{Z}_D$ can be multiplied in $O(m^\theta)$ operations from $\mathbb{Z}_D$. Using standard matrix multiplication $\theta=3$, but better algorithms [26] allow for $\theta = 2.38$.

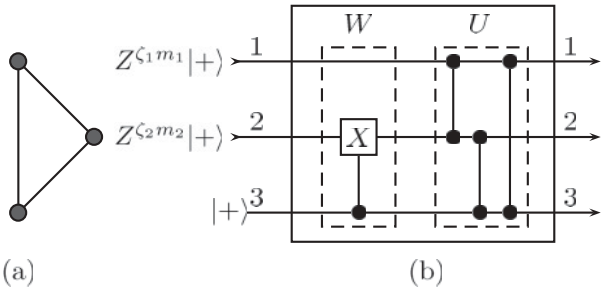

FIG. 1. (a) The graph state used in the example. (b) The encoding circuit: the input states $Z_1^{\zeta_1 m_1} Z_2^{\zeta_2 m_2}|{+}{+}\rangle$ that correspond to the trivial code $\mathcal{C}_0$ are mapped by W to $\mathcal{C}$, then U entangles the qudits. Here $m_1=2$, $m_2=3$, and ζ_j are integers such that $0\leqslant\zeta_j\leqslant d_j-1$, with $d_1=3$, $d_2=2$.

For the example above, the sequence

$$\begin{pmatrix} 4 & 3 & 3 \\ 0 & 3 & 3 \end{pmatrix} \to \begin{pmatrix} 4 & 0 & 0 \\ 0 & 3 & 3 \end{pmatrix} \to \begin{pmatrix} 4 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} = \mathbf{s} \tag{33}$$

proceeds by adding the second row of **f** to the first (mod 6), then the second column to the third column, and finally multiplying the first row by 5 (which is invertible mod 6). The final step is needed so that the diagonal elements divide D: $m_1=2$, $m_2=3$, so that $d_1=3$ and $d_2=2$. Thus we arrive at the trivial coding group

$$\mathcal{C}_0 = \langle Z_1^2, Z_2^3 \rangle, \tag{34}$$

isomorphic to $\mathcal{C}$ in (30).

Since the procedure for reducing a matrix to Smith normal form is quite general, the procedure illustrated in this example can be applied to any coding group $\mathcal{C}$, as defined following (26), to find a corresponding trivial coding group $\mathcal{C}_0$. The row operations change the collection of generators but not the coding group that they generate; i.e., the final collection of K rows is the same. The column operations, on the other hand, produce a different, but isomorphic, coding group, and one can think of these as realized by a unitary operator W which is a product of various SWAP, CNOT, and S_q gates, so that

$$\mathcal{C} = W\mathcal{C}_0 W^\dagger, \tag{35}$$

that is, conjugation by W maps each operator in $\mathcal{C}_0$ to its counterpart in $\mathcal{C}$. In our example, $W = \text{CNOT}_{32}$ is the only column operation, the second arrow in (33), and represents the first step in the encoding circuit for this example [Fig. 1(b)]. It is left as an exercise to check that this relates the generators in (30) and (34) through (35). Table III indicates how different matrix column operations are related to the corresponding gates in the encoding circuit.

The overall encoding operation

$$|\mathbf{c}_j\rangle = U W |\mathbf{c}_j^0\rangle \tag{36}$$

starting with the trivial code on the trivial graph $(\mathcal{C}_0, |G_0\rangle)$ and ending with the desired code $(\mathcal{C}, |G\rangle)$ is shown for our example in Fig. 1(b) for the case of a graph indicated in (a) in this figure. It is important to notice that both W and U, and therefore their product, are Clifford operators, unitaries that under conjugacy map Pauli products to Pauli products. This follows from the fact that the gates in Table III are Clifford gates and will allow us in what follows to extend arguments

TABLE III. The correspondence between matrix column operations in $\mathbb{Z}_D$ and conjugation by Clifford gates. For the CNOT gate, the first qudit a is the control and the second qudit b is the target.

Matrix operation in $\mathbb{Z}_D$	Clifford conjugation
Interchange of columns a and b	SWAP_{ab}
Multiplication of column a by invertible integer q	S_q on qudit a
Addition of m times column b to column a	$(\mathrm{CNOT}_{ab})^m$

that are relatively straightforward for trivial codes on trivial graphs to more general additive graph codes.

C. The information group

In this section we define the *information group* that plays a central role in the isomorphism theorem in Sec. V below. The basic strategy is most easily understood in terms of $C_0 = (\mathcal{C}_0, |G_0\rangle)$, the trivial code on the trivial graph. However, because the overall encoding map UW in (36) is a Clifford operation mapping Pauli products to Pauli products, various results that apply to C_0 can be immediately translated to the general graph code $C = (\mathcal{C}, |G\rangle)$ we are interested in, and for this reason most of the formulas valid for both are written in the form valid for C even if the derivations are based on C_0.

The pointwise stabilizer[1] of C_0, the subgroup of operators from $\mathcal{P}_n$ that leave every codeword $|\mathbf{c}_j^0\rangle$ unchanged, is given by

$$\mathcal{S}_0 = \{X^{\mathbf{x}} : \mathbf{x} = (\eta_1 d_1, \eta_2 d_2, \ldots, \eta_k d_k, x_{k+1}, \ldots, x_n)\}, \quad (37)$$

where the d_j are defined in (29), η_j is any integer between 0 and $m_j - 1$, and the x_j for $j > k$ are arbitrary integers between 0 and $D - 1$. That this is correct can be seen as follows. First, Pauli products belonging to $\mathcal{S}_0$ cannot contain Z_j operators, for such operators map each codeword onto an orthogonal state. On the other hand, every $X_j^{x_j}$ leaves $|G_0\rangle$, (21), unchanged, so it belongs to $\mathcal{S}_0$ if and only if it commutes with $Z_j^{m_j}$, which means $x_j m_j$ must be a multiple of D, or x_j a multiple of d_j, see (29). Thus elements of $\mathcal{S}_0$ commute with elements of $\mathcal{C}_0$ (28). Since its operators cannot alter the phases of the codewords, no additional factors of ω^λ are allowed, and thus $\mathcal{S}_0$ is given by (37). The stabilizer of the (nontrivial) code C is then the isomorphic group $\mathcal{S}$ obtained using the unitary UW of (36):

$$\mathcal{S} = (UW)\mathcal{S}_0(UW)^\dagger \equiv \{(UW)s(UW)^\dagger : s \in \mathcal{S}_0\}, \quad (38)$$

a collection of Pauli products because the unitary UW, as remarked earlier, is a Clifford unitary. The order of $\mathcal{S}_0$, and thus of $\mathcal{S}$, is given by

$$|\mathcal{S}| = D^{n-k}\prod_{j=1}^{k} m_j = \frac{D^n}{\prod_{j=1}^{k} d_j} = \frac{D^n}{|\mathcal{C}|} = \frac{D^n}{K}. \quad (39)$$

Next define the subgroup $\mathcal{W}$ of $\mathcal{P}_n$ as

$$\mathcal{W} = \langle \mathcal{S}^G, \mathcal{C}\rangle \quad (40)$$

generated by operators belonging to the stabilizer $\mathcal{S}^G$ of the graph state or to the coding group $\mathcal{C}$, and we denote it by $\mathcal{W}_0 = \langle \mathcal{S}_0^G, \mathcal{C}_0\rangle$ in the case of the trivial code. The elements of $\mathcal{S}_0$ commute with those of $\mathcal{S}_0^G$ (both are Abelian and the former is a subgroup of the latter), and also with those of $\mathcal{C}_0$, as noted above. As group properties are preserved under the UW map, as in (38), we conclude that all elements in $\mathcal{S}$ commute with those in $\mathcal{W}$, even though $\mathcal{W}$ is not (in general) Abelian, and hence $\mathcal{S}$ is a normal subgroup of $\mathcal{W}$. Now define the *abstract information group* as the quotient group

$$\overline{\mathcal{G}} = \mathcal{W}/\mathcal{S} = \langle \mathcal{S}^G, \mathcal{C}\rangle/\mathcal{S} \quad (41)$$

consisting of cosets of $\mathcal{S}$, written as $g\mathcal{S}$ or $\mathcal{S}g$ for g in $\mathcal{W}$. Note that because any element g of $\mathcal{W}$ is a Pauli product, $g^D = I$ is the identity, and the order of g is either D or an integer that divides D. Consequently the order of any element of $\overline{\mathcal{G}}$ is also D or an integer that divides D.

To understand the significance of $\overline{\mathcal{G}}$ consider a trivial code on a single qudit, with

$$\mathcal{C}_0 = \langle Z_1^{m_1}\rangle, \quad \mathcal{S}_0^G = \langle X_1\rangle, \quad \mathcal{S}_0 = \langle X_1^{d_1}\rangle. \quad (42)$$

The elements of $\overline{\mathcal{G}}_0$ can be worked out using its identity $\bar{I}$ and the generators $\bar{X}$ and $\bar{Z}$:

$$\begin{aligned} \bar{I} &= \mathcal{S}_0 = \{I_1, X_1^{d_1}, X_1^{2d_1}, \ldots\}, \\ \bar{X} &= X_1\mathcal{S}_0 = \{X_1, X_1^{d_1+1}, X_1^{2d_1+1}, \ldots\}, \\ \bar{Z} &= Z_1^{m_1}\mathcal{S}_0 = \{Z_1^{m_1}, Z_1^{m_1}X_1^{d_1}, \ldots\}. \end{aligned} \quad (43)$$

It is evident that the cosets $\bar{X}$, $\bar{X}^2 = X_1^2\mathcal{S}_0$ and so forth up to $\bar{X}^{d_1-1}$ are distinct, whereas $\bar{X}^{d_1} = \bar{I} = \mathcal{S}_0$. The same is true for powers of $\bar{Z}$. Furthermore,

$$\bar{X}\bar{Z} = X_1 Z_1^{m_1}\mathcal{S}_0 = \omega^{m_1} Z_1^{m_1} X_1\mathcal{S}_0 = \bar{\omega}\bar{Z}\bar{X}, \quad (44)$$

with $\bar{\omega} = \omega^{m_1} = e^{2\pi i/d_1}$. Thus $\overline{\mathcal{G}}_0$ is generated by operators $\bar{X}$ and $\bar{Z}$ that satisfy (8) with D replaced by d_1, which is to say the corresponding group is what one would expect for a qudit of dimension d_1. The same argument extends easily to the trivial code on k carriers produced by $\mathcal{C}_0$ [see (28)]: $\overline{\mathcal{G}}_0$ is isomorphic to the group of Pauli products on a set of qudits of dimension $d_1, d_2, \ldots, d_k$. The same structure is inherited by the abstract information group $\overline{\mathcal{G}}$ for the code $C = (\mathcal{C}, |G\rangle)$ obtained by applying the UW map as in (38).

The abstract information group $\overline{\mathcal{G}}$ is isomorphic to the *information group* $\mathcal{G}$ of *information operators* acting on the coding space $\mathcal{H}_C$ and defined in the following way. Its identity is the operator

$$P = |\mathcal{S}|^{-1}\Sigma(\mathcal{S}) = |\mathcal{S}|^{-1}\sum_{s\in\mathcal{S}} s, \quad (45)$$

where $\Sigma(\mathcal{A})$ denotes the sum of the operators that make up a collection $\mathcal{A}$. In fact, P is just the projector onto $\mathcal{H}_C$, as

[1] Also called the fixer or fixator. It is important to distinguish this subgroup from the group theoretical notion of the stabilizer of the coding space in the sense of the subgroup of $\mathcal{P}_n$ that maps the coding space onto itself without necessarily leaving the individual vectors fixed. As we shall not employ the latter, it should cause no confusion if we hereafter follow the usual convention in quantum codes and omit "pointwise," even though retaining it would add some precision.

can be seen as follows. Since $\mathcal{S}$ is a group, $P^2 = P$; and since a group contains the inverse of every element, and $s \in \mathcal{S}$ is unitary (a Pauli product), $P^\dagger = P$. These two conditions mean that P is a projector onto some subspace of $\mathcal{H}_n$. Since $\mathcal{S}$ is the (pointwise) stabilizer of the coding space each s in $\mathcal{S}$ maps a codeword onto itself, and thus P maps each codeword to itself. Consequently, all the codewords lie in the space onto which P projects. Finally, the rank of P is

$$\mathrm{Tr}[P] = D^n/|\mathcal{S}| = |\mathcal{C}| = K \tag{46}$$

[see (39)], since the trace of every s in $\mathcal{S}$ is zero except for the identity with trace D^n. (Note that while $\mathcal{P}_n$ contains the identity multiplied by various phases, only the identity operator occurs in $\mathcal{S}$.) Therefore P projects onto $\mathcal{H}_C$, and is given by the formula

$$P = \sum_{j=1}^{K} |\mathbf{c}_j\rangle\langle\mathbf{c}_j|. \tag{47}$$

The other information operators making up the information group $\mathcal{G} = \{\hat{g}\}$ are formed in a similar way from the different cosets making up $\mathcal{W}/\mathcal{S}$:

$$\hat{g} = |\mathcal{S}|^{-1}\Sigma(g\mathcal{S}) = gP = PgP = P\hat{g}P. \tag{48}$$

That is, for each coset form the corresponding sum of operators and divide by the order of the stabilizer $\mathcal{S}$. The second and third equalities in (48) reflect the fact that the product of the cosets $\mathcal{S}$ and $g\mathcal{S}$ in either order is $g\mathcal{S}$, which is to say P forms the group identity of $\mathcal{G}$. They also tell us that the operators that make up $\mathcal{G}$ act only on the coding space, mapping $\mathcal{H}_C$ onto itself, and give zero when applied to any element of $\mathcal{H}_n$ in the orthogonal complement of $\mathcal{H}_C$. Because $\mathcal{S}$ is a normal subgroup of $\mathcal{W}$, products of operators of the form (48) mirror the products of the corresponding cosets, so the map from the abstract $\overline{\mathcal{G}}$ to the group $\mathcal{G}$ is a homomorphism. That it is actually an isomorphism is a consequence of the following, proved in Appendix A:

Lemma 1. Let $\mathcal{R}$ be a linearly independent collection of Pauli product operators that form a subgroup of $\mathcal{P}_n$, and for a Pauli product p let $p\mathcal{R} = \{pr : r \in \mathcal{R}\}$. Then we have the following.

(i) The operators in $p\mathcal{R}$ are linearly independent and

(ii) If p and q are two Pauli products, one or the other of the following two mutually exclusive possibilities obtains:

(α)

$$p\mathcal{R} = e^{i\phi}q\mathcal{R} \tag{49}$$

in the sense that each operator in $p\mathcal{R}$ is equal to $e^{i\phi}$ times an operator in $q\mathcal{R}$.

(β) the union $p\mathcal{R} \cup q\mathcal{R}$ is a collection of $2|\mathcal{R}|$ linearly independent operators.

Since the collection of Pauli products $\mathcal{Q}_n$ with fixed phase forms a basis of $\mathcal{L}(\mathcal{H}_n)$, a collection of Pauli products can be linearly *dependent* if and only if it contains both an operator and that operator multiplied by some phase. As the (pointwise) stabilizer $\mathcal{S}$ leaves each codeword unchanged, the corresponding operators are linearly independent, and the lemma tells us that distinct cosets $g\mathcal{S} \neq h\mathcal{S}$ give rise to distinct operators $\hat{g} \neq \hat{h}$. Either $g\mathcal{S} = e^{i\phi}h\mathcal{S}$, in which case $\hat{g} = e^{i\phi}\hat{h} \neq \hat{h}$ (since if $e^{i\phi} = 1$ the cosets are identical) or else the $g\mathcal{S}$ operators are linearly independent of the $h\mathcal{S}$ operators, and therefore $\hat{g}$ and $\hat{h}$ are linearly independent. Consequently, the homomorphic map from $\overline{\mathcal{G}}$ to $\mathcal{G}$ is a bijection, and the two groups are isomorphic.

The single-qudit example considered in (42) provides an example of how $\overline{\mathcal{G}}$ and $\mathcal{G}$ are related. In this case the projector

$$P_0 = (1/m_1)\left(I_1 + X_1^{d_1} + \cdots\right) \tag{50}$$

projects onto the subspace spanned by $|+\rangle$, $Z_1^{m_1}|+\rangle$, $Z_1^{2m_1}|+\rangle, \ldots$. While each of the operators that make up a coset such as $\bar{X}$ in (43) is unitary, their sum, an operator times P_0, is no longer unitary, though when properly normalized it acts as a unitary on the subspace onto which P_0 projects. That the different sums of operators making up the different cosets are distinct is in this case evident from inspection without the need to invoke Lemma 1.

Let us summarize the main results of this subsection. For an additive graph code C we have defined the information group $\mathcal{G}$ of operators acting on the coding subspace $\mathcal{H}_C$, whose group identity is the projector P onto $\mathcal{H}_C$. It is isomorphic to the group of Pauli products acting on a tensor product of qudits of dimensions $d_1, d_2, \ldots, d_k$, which can be thought of as the input to the code, see Sec. IV B. Each element $\hat{g}$ of $\mathcal{G}$ is of the form $P\hat{g}P$, so as an operator on $\mathcal{H}_n$ it commutes with P and yields zero when applied to any vector in the orthogonal complement of $\mathcal{H}_C$. The dimension of $\mathcal{H}_C$ is $K = d_1 d_2 \cdots d_k$, the size of the code, and hence the elements of $\mathcal{G}$ span the space of linear operators $\mathcal{L}(\mathcal{H}_C)$ on $\mathcal{H}_C$.

V. SUBSETS OF CARRIERS AND THE ISOMORPHISM THEOREM

A. Subsets of carriers

Before stating the isomorphism theorem, which is the principal technical result of this paper, let us review some facts established in Sec. IV. The additive graph code $(\mathcal{C}, |G\rangle)$ we are interested in can be thought of as arising from an encoding isometry that carries the channel input onto a subspace $\mathcal{H}_C$ of the n-qudit carrier space $\mathcal{H}_n$, as in Fig. 1. This isometry, as explained in Sec. II in connection with (4), constitutes a perfect quantum channel, and thus all the information of interest can be said to be located in the $\mathcal{H}_C$ subspace, where it is represented by the information group $\mathcal{G}$, a multiplicative group of operators for which the projector P on $\mathcal{H}_C$ is the group identity, and which as a group is isomorphic to the abstract information group $\overline{\mathcal{G}}$ defined in (41).

We are interested in what kinds of information are available in some subset B of the carriers, where $\bar{B}$ denotes the complementary set. For this purpose it is natural to consider the partial traces over $\bar{B}$, i.e., the traces down to the Hilbert space $\mathcal{H}_B$, of the form

$$g_B = N^{-1}\mathrm{Tr}_{\bar{B}}[\hat{g}], \tag{51}$$

where $\hat{g}$ is an element of the information group $\mathcal{G}$, and the positive constant N is defined in (58) below. In those cases in which $g_B = 0$ the $\mathcal{J}(\hat{g})$ information has disappeared and is not available in the subset B, so we shall be interested in those $\hat{g}$ for which the partial trace does not vanish, that is to say in

the elements of the *subset information group*

$$\mathcal{G}^B = \{\hat{g} \in \mathcal{G} : \mathrm{Tr}_{\bar{B}}[\hat{g}] \neq 0\}. \tag{52}$$

We show below that $\mathcal{G}^B$ is a subgroup of $\mathcal{G}$, thus justifying its name, and that it is isomorphic to the group $\mathcal{G}_B$ of nonzero operators of the form g_B defined in (51). To actually determine which elements of $\mathcal{G}$ belong to $\mathcal{G}^B$ one needs to take partial traces of the $\hat{g} \in \mathcal{G}$ to see which of them do not trace down to zero. In Appendix C we present an efficient linear algebra algorithm based on solving systems of linear equations mod D that can find $\mathcal{G}^B$ in $O(K^2 n^\theta)$ operations from $\mathbb{Z}_D$ where θ is defined in Sec. IV B.

If an operator A on the full Hilbert space $\mathcal{H}_n$ of the n carriers can be written as a tensor product of an operator on $\mathcal{H}_B$ times the identity operator $I_{\bar{B}}$ on $\mathcal{H}_{\bar{B}}$ we shall say that A is *based in* B. Let $\mathcal{B}$ be the collection of all operators on $\mathcal{H}_n$ that are based in B. Obviously, $\mathcal{B}$ is closed under sums, products, and scalar multiplication. In addition the partial trace $\mathrm{Tr}_{\bar{B}}[A]$ of an operator A in $\mathcal{B}$ is "essentially the same" operator, apart from normalization in the sense that

$$A = D^{-|\bar{B}|} \cdot \mathrm{Tr}_{\bar{B}}[A] \otimes I_{\bar{B}}. \tag{53}$$

If $A \notin \mathcal{B}$ is a Pauli product, then its partial trace over $\bar{B}$ vanishes, since $\mathrm{Tr}[X]$ and $\mathrm{Tr}[Z]$ and their powers (when not equal to I) are zero. Consequently, the partial trace over $\bar{B}$ of $\Sigma(g\mathcal{S})$ in (48) is the same as the partial trace of $\Sigma[(g\mathcal{S}) \cap \mathcal{B}]$, which suggests that it is useful to consider the properties of collections of Pauli operators of the form $(g\mathcal{S}) \cap \mathcal{B}$ with g an element of $\mathcal{W}$. The following result, proved in Appendix A, turns out to be useful.

Lemma 2. Let g, h be two arbitrary elements of $\mathcal{W}$, and let $\mathcal{B}$ be the collection of operators with base in B.

(i) The set $(g\mathcal{S}) \cap \mathcal{B}$ is empty if and only if $(g^{-1}\mathcal{S}) \cap \mathcal{B}$ is empty.

(ii) Every nonempty set of the form $(g\mathcal{S}) \cap \mathcal{B}$ contains precisely

$$M = |\mathcal{S} \cap \mathcal{B}| \geqslant 1 \tag{54}$$

elements.

(iii) Two nonempty sets $(g\mathcal{S}) \cap \mathcal{B}$ and $(h\mathcal{S}) \cap \mathcal{B}$ are either identical, which means $g\mathcal{S} = h\mathcal{S}$ and $\Sigma[(g\mathcal{S}) \cap \mathcal{B}] = \Sigma[(h\mathcal{S}) \cap \mathcal{B}]$, or else they have no elements in common and the operators $\Sigma[(g\mathcal{S}) \cap \mathcal{B}]$ and $\Sigma[(h\mathcal{S}) \cap \mathcal{B}]$ are distinct.

(iv) If both $(g\mathcal{S}) \cap \mathcal{B}$ and $(h\mathcal{S}) \cap \mathcal{B}$ are nonempty, their product as sets, including multiplicity, is given by

$$[(g\mathcal{S}) \cap \mathcal{B}] \cdot [(h\mathcal{S}) \cap \mathcal{B}] = M[(gh\mathcal{S}) \cap \mathcal{B}]. \tag{55}$$

By (55) we mean the following. The product (on the left) of any operator from the collection $(g\mathcal{S}) \cap \mathcal{B}$ with another operator from the collection $(h\mathcal{S}) \cap \mathcal{B}$ belongs to the collection $(gh\mathcal{S}) \cap \mathcal{B}$ (on the right), and every operator in $(gh\mathcal{S}) \cap \mathcal{B}$ can be written as such a product in precisely M different ways.

We are now in a position to state and prove our central result.

B. Isomorphism theorem

Theorem 3 (Isomorphism). Let C be an additive graph code with information group $\mathcal{G}$, let P be the projector onto the coding space $\mathcal{H}_C$, and let B be some subset of the carrier qudits. Then the collection $\mathcal{G}^B$ of members of $\mathcal{G}$ with nonzero partial trace down to B (52) is a subgroup of the information group $\mathcal{G}$, and the mapping $\hat{g} \to g_B$ in (51) carries $\mathcal{G}^B$ to an isomorphic group $\mathcal{G}_B$ of nonzero operators on $\mathcal{H}_B$. Furthermore we have the following.

(i) If $\hat{g}$ and $\hat{h}$ are any two elements of $\mathcal{G}^B$, then

$$\mathrm{Tr}_{\bar{B}}[\hat{g}\hat{h}] = \mathrm{Tr}_{\bar{B}}[\hat{g}]\mathrm{Tr}_{\bar{B}}[\hat{h}]/N \quad \text{or} \quad (gh)_B = g_B h_B. \tag{56}$$

(ii) If $\hat{g} \neq \hat{h}$ are distinct elements of $\mathcal{G}^B$, $g_B \neq h_B$ are distinct elements of $\mathcal{G}_B$.

(iii) The identity element

$$P_B := \mathrm{Tr}_{\bar{B}}[P]/N, \tag{57}$$

of $\mathcal{G}_B$ is a projector onto a subspace of $\mathcal{H}_B$ (possibly the whole space) with rank equal to $\mathrm{Tr}[P]/N = K/N$.

The normalization constant N is given as

$$N := |\mathcal{S} \cap \mathcal{B}| \cdot D^{|\bar{B}|}/|\mathcal{S}|, \tag{58}$$

where $\mathcal{B}$ are the operators based in B.

Proof. The proof is a consequence of Lemma 2 and the following observations. The trace $\mathrm{Tr}_{\bar{B}}[\hat{g}]$ in (51) is, apart from a constant, the trace of $\Sigma[(g\mathcal{S}) \cap \mathcal{B}]$, and is zero if $(g\mathcal{S}) \cap \mathcal{B}$ is empty. If the collection $(g\mathcal{S}) \cap \mathcal{B}$ is not empty, then by Lemma 1 it consists of a collection of linearly independent operators, and the trace of its sum cannot vanish. Thus there is a one-to-one [see part (iii) of Lemma 2] correspondence between nonempty sets of the form $(g\mathcal{S}) \cap \mathcal{B}$ and the elements $\hat{g}$ in $\mathcal{G}^B$. Then (i) and (iv) of Lemma 2 imply both that $\mathcal{G}^B$ is a group and also that the map from $\mathcal{G}^B$ to $\mathcal{G}_B$ is a homomorphism, whereas (ii) shows that this is actually an isomorphism: $g_B = h_B$ is only possible when $g\mathcal{S} = h\mathcal{S}$. That N in (58) is the correct normalization follows from (54), (55), and (48). ■

A significant consequence of Theorem 3 is the following result on the presence and absence of information in the subset B, using the terminology of Sec. II:

Theorem 4. Let C be an additive graph code on n carrier qudits, with information group $\mathcal{G}$. Let B be a subset of the carrier qudits, $\mathcal{G}^B$ the corresponding subset information group, and $\mathcal{J}(\hat{g})$ the type of information corresponding to $\hat{g}$ (as defined in Sec. II). Then we have the following.

(i) The $\mathcal{J}(\hat{g})$ type of information is perfectly present in B if and only if $\hat{g} \in \mathcal{G}^B$.

(ii) The $\mathcal{J}(\hat{g})$ type of information is absent from B if and only if $\hat{g}^k \notin \mathcal{G}^B$ for all integers k between 1 and $D-1$.

(iii) All information is perfectly present in B if and only if $\mathcal{G}^B = \mathcal{G}$.

(iv) All information is absent from B if and only if $\mathcal{G}^B$ consists entirely of scalar multiples of the identity element P of $\mathcal{G}$.

The proof of the theorem can be found in Appendix B. Statement (iii) is useful because the check of whether there is a perfect quantum channel from the input to B involves a finite group $\mathcal{G}$; one does not have to consider all normal operators of the form (2). Statement (ii) deserves further comment. If D is prime then the order of any element of the Pauli group (apart from the identity) is D see the remark following (9). The same is true of elements of the quotient group $\overline{\mathcal{G}}$ (41) and thus of members $\hat{g}$ of the isomorphic group $\mathcal{G}$. Consequently,

for any k in the interval $1 < k < D$, there is some m such that $1 = km \bmod D$, which means $\hat{g} = (\hat{g}^k)^m$. And since $\mathcal{G}^B$ is a group, $\hat{g}^k \in \mathcal{G}^B$ implies $\hat{g} \in \mathcal{G}^B$. Thus when D is prime, $\hat{g} \notin \mathcal{G}^B$ is equivalent to $\hat{g}^k \notin \mathcal{G}^B$ for all integers k between 1 and $D-1$, and the latter can be replaced by the former in statement (ii). However, when D is composite it is quite possible to have $\mathrm{Tr}_{\bar{B}}[\hat{g}] = 0$ but $\mathrm{Tr}_{\bar{B}}[\hat{g}^{k'}] \neq 0$ for some k' larger than 1 and less than D; see the example below. In this situation we can still say that $\mathcal{J}(\hat{g}^{k'})$ is perfectly present, but it is not true that $\mathcal{J}(\hat{g})$ is absent. One can regard the type $\mathcal{J}(\hat{g})$ as a *refinement* of $\mathcal{J}(\hat{g}^{k'})$, and as explained in Sec. II, although the coarse-grained $\mathcal{J}(\hat{g}^{k'})$ information is perfectly present in B, the additional information associated with the refinement is not.

As an example, suppose $\hat{g}$ has a spectral decomposition

$$\hat{g} = J_0 + \mathrm{i}J_1 - J_2 - \mathrm{i}J_3, \tag{59}$$

with the J_j orthogonal projectors such that

$$\mathrm{Tr}_{\bar{B}}[J_0] = \mathrm{Tr}_{\bar{B}}[J_2] \neq \mathrm{Tr}_{\bar{B}}[J_1] = \mathrm{Tr}_{\bar{B}}[J_3]. \tag{60}$$

Then $\mathrm{Tr}_{\bar{B}}[\hat{g}] = 0$, whereas

$$\hat{g}^2 = (J_0 + J_2) - (J_1 + J_3), \tag{61}$$

and thus $\mathrm{Tr}_{\bar{B}}[\hat{g}^2] \neq 0$. Thus $\hat{g}^2$ is an element of $\mathcal{G}^B$, whereas $\hat{g}$ is not, and so the coarse grained $\mathcal{J}(\hat{g}^2)$ information corresponding to the decomposition on the right side of (61) is present in B, while the further refinement corresponding to the right side of (59) is not. Precisely this structure is produced by a graph code on two carriers of dimension $D = 4$, with graph state $|G\rangle = |{+}{+}\rangle$, coding group $\mathcal{C} = \langle Z_1 Z_2 \rangle$, information group $\mathcal{G} = \langle X_1 P, Z_1 Z_2 P \rangle$, coding space projector

$$P = \left(I + X_1 X_2^3 + X_1^2 X_2^2 + X_1^3 X_2\right)/4, \tag{62}$$

and

$$\hat{g} = X_1 P = |\bar{0}\bar{0}\rangle\langle\bar{0}\bar{0}| + \mathrm{i}|\bar{1}\bar{2}\rangle\langle\bar{1}\bar{2}| - |\bar{2}\bar{0}\rangle\langle\bar{2}\bar{0}| - \mathrm{i}|\bar{3}\bar{2}\rangle\langle\bar{3}\bar{2}|, \tag{63}$$

where $|\bar{j}\rangle = Z^j|{+}\rangle$ are the eigenvectors of the X operator.

C. Information flow

At this point let us summarize how we think about information "flowing" from the input via the encoding operation into a subset B of the code carriers. At the input the information is represented by the quotient group $\overline{\mathcal{G}}_0 = \mathcal{W}_0/\mathcal{S}_0$ [see (41)] or more concretely by the isomorphic group $\mathcal{G}_0$ of operators generated by the cosets, as in (48). The encoding operation UW [see (36) and (38)] maps $\overline{\mathcal{G}}_0$ to the analogous $\overline{\mathcal{G}} = \mathcal{W}/\mathcal{S}$ associated with the code C, and likewise $\mathcal{G}_0$ to the group of operators $\mathcal{G}$ acting on the coding space $\mathcal{H}_C$. Tracing away the complement $\bar{B}$ of B maps some of the $\hat{g}$ operators of $\mathcal{G}$ to zero, and the remainder form the subset information group $\mathcal{G}^B$. Applying the inverse UW map to $\mathcal{G}^B$ gives $\mathcal{G}_0^B$, a subgroup of $\mathcal{G}_0$ that tells us what types of information at the input (i.e. before the encoding) are available in the subset of carriers B. This is illustrated by various examples in the next section.

VI. EXAMPLES

A. General principles

In this section we apply the principles developed earlier in the paper to some simple $[[n, k, \delta]]_D$ additive graph codes, where n is the number of qudit carriers, each of dimension D, the dimension of the coding space $\mathcal{H}_C$ is $K = D^k$, and δ is the distance of the code; see Chap. 10 of [27] for a definition of δ. We shall be interested in the subset information group $\mathcal{G}^B$, (52), that represents the information about the input that is present in the subset B of carriers. Rather than discussing $\mathcal{G}^B$ or its traced down counterpart $\mathcal{G}_B$, it will often be simpler to use $\mathcal{G}_0^B$, the subset information group referred back to the channel input (see Sec. V C), and in this case we add an initial subscript 0 to operators: X_{01} means the X operator on the first qudit of the input. Since all three groups are isomorphic to one another, the choice of which to use in any discussion is a matter of convenience. (In the examples below for the sake of brevity we sometimes omit a term $e^{\mathrm{i}\phi} I$ from the list of generators of $\mathcal{G}_0^B$.)

Before going further it is helpful to list some general principles of quantum information that apply to all codes, and which can simplify the analysis of particular examples, or give an intuitive explanation of why they work. In the following statements "information" always means information about the input which has been encoded in the coding space through some isometry.

1. If all information is perfectly present in B, then all information is absent from $\bar{B}$.

2. If all information is absent from $\bar{B}$ then all information is perfectly present in B.

3. If the information about some orthonormal basis (i.e., the type corresponding to this decomposition of the identity) is perfectly present in B, then the information about a mutually unbiased basis is absent from $\bar{B}$.

4. If two types of information that are "sufficiently incompatible" are both perfectly present in B, then all information is perfectly present in B. In particular this is so when the two types are associated with mutually unbiased bases.

5. For a code of distance δ all information is absent from any B if $|B| < \delta$, and all information is perfectly present in B if $|B| > n - \delta$.

Items 1, 2, 3, and 4 correspond to the No Splitting, Somewhere, Exclusion, and Presence theorems of [20], which also gives weaker conditions for "sufficiently incompatible." The essential idea behind 5 is found in Sec. III A of [28].[2]

B. One encoded qudit

It was shown in [12] that a $[[5, 1, 3]]_D$ code exists for all D. Here we consider the graph version [13] where the coding group is

$$\mathcal{C} = \langle Z_1 Z_2 Z_3 Z_4 Z_5 \rangle \tag{64}$$

and the graph state is shown in Fig. 2(a). Our formalism shows that, whatever the value of D, there are only two possibilities.

[2]It is shown in [28] that if noise only affects a certain subset $\bar{B}$ of the carriers with $|\bar{B}| < \delta$, then the errors can be corrected using the complementary set B. In our notation this is equivalent to saying that all the information is in B.

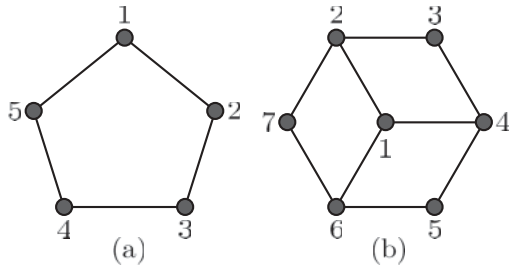

FIG. 2. (a) The graph state for the $[[5, 1, 3]]_D$ code. (b) The graph state for the Steane $[[7, 1, 3]]_2$ code.

When $|B|$ is 1 or 2, $\mathcal{G}^B$ is the just the group identity, the projector P on the coding space, so all information is absent, whereas if $|B|$ is 3, 4, or (obviously) 5, $\mathcal{G}^B = \mathcal{G}$, so the subsystem B is the output of a perfect quantum channel. To be sure, these results also follow from principle 5 in the above list, given that $\delta = 3$ for this code.

The Steane $[[7, 1, 3]]_2$ code, a graphical version of which [29] has a coding group

$$\mathcal{C} = \langle Z_3 Z_5 Z_7 \rangle \tag{65}$$

for the graph state shown in Fig. 2(b), is more interesting in that while principles 5 ensures that all $|B| \leqslant 2 = \delta - 1$ subsets of carriers contain zero information and all $|B| \geqslant 5 = n - \delta + 1$ subsets contain all the information, one qubit, it leaves open the question of what happens when $|B| = 3$ or 4. We find that all information is perfectly present when B is $\{1, 2, 5\}$, $\{1, 3, 6\}$, $\{1, 4, 7\}$, $\{2, 3, 4\}$, $\{2, 6, 7\}$, $\{4, 5, 6\}$, or $\{3, 5, 7\}$—representing three different symmetries in terms of the graph in the figure—and absent for all other cases of $|B| = 3$. Therefore all information is absent from the $|B| = 4$ subsets which are complements of the seven just listed and perfectly present in all others of size $|B| = 4$. So far as we know, generalizations of this code to $D > 2$ have not been studied.

A simple code in which a specific type of information is singled out is $[[n, 1, 1]]_D$ generated by

$$\mathcal{C} = \langle Z_1 Z_2 \cdots Z_n \rangle \tag{66}$$

on the *complete graph*, illustrated in Fig. 3(b) for $n = 6$. Whereas all information is (of course) present when $|B| = n$, it turns out that for any subset B with $1 \leqslant |B| < n$ one has $\mathcal{G}_0^B = \langle X_{01} Z_{01} \rangle$, i.e., the Abelian group consisting of all powers of the operator $X_1 Z_1$ on the input qudit. Thus the information is "classical," corresponding to that decomposition of the input identity that diagonalizes $X_1 Z_1$. The intuitive explanation for this situation is that this $X_1 Z_1$ type of information is separately copied as an ideal classical channel [see (6)] to each of the carrier qudits, and as a consequence other mutually unbiased types of information are ruled out by principle 3. This, of course, is typical of "classical" information, which can always be copied.

A more interesting example in which distinct types of information come into play is the bar graph [Fig. 3(a)], in which n qudits are divided up into $p = n/2$ pairs or "bars," and the code is generated by

$$\mathcal{C} = \langle Z_1 Z_2 \cdots Z_n \rangle. \tag{67}$$

Let us say that a subset of carriers B has property I if the corresponding subgraph contains at least one of bars and property II if it contains at least one qudit from each of the bars. Then the following holds:

(i) If B has property I but not II, $\mathcal{G}_0^B = \langle X_{01} \rangle$, an Abelian group.

(ii) If B has property II but not I, $\mathcal{G}_0^B = \langle X_{01}^p Z_{01} \rangle$, another Abelian group.

(iii) If B has both property I and property II, all information (one qudit) is perfectly present.

(iv) When B has neither property I nor II, all information is absent.

While both (i) and (ii) are "classical" in an appropriate sense and indeed represent an ideal classical channel, the two Abelian groups do not commute with each other, so the two types of information are incompatible, and it is helpful to distinguish them. Case (iii) illustrates principle 4, since X_{01} and $X_{01}^p Z_{01}$ (whatever the value of p) correspond to mutually unbiased bases. In case (iv) the complement $\bar{B}$ of B possesses both properties I and II, and therefore contains all the information, so its absence from B is an illustration of principle 1.

C. Two encoded qudits

Consider a $[[4, 2, 2]]_D$ code based on the graph state shown in Fig. 4 whose coding group

$$\mathcal{C} = \langle Z_1 Z_2, Z_3 Z_4 \rangle, \tag{68}$$

employs two generators of order D and thus encodes two qudits. Note that while the graph state has the symmetry of a square the coding group has a lower symmetry corresponding to the different types of nodes employed in the figure.

Let us begin with the qubit case $D = 2$. Our analysis shows that when $|B| = 1$ all information is absent, and thus for $|B| \geqslant 3$ all information is present, consistent with the fact that this

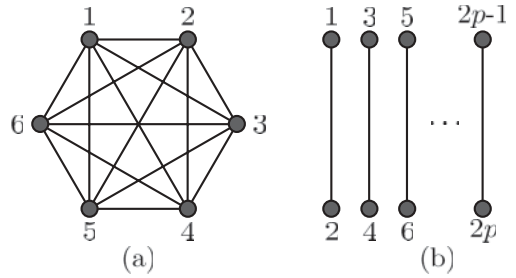

FIG. 3. (a) Complete graph (on six qudits). (b) Bar graph with $n = 2p$ carriers and p bars.

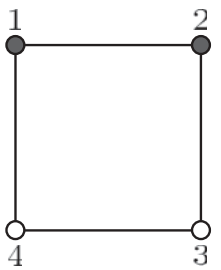

FIG. 4. The graph state of the $[[4, 2, 2]]_D$ code.

code has $\delta = 2$ [8] (see principle 5). Thus the interesting cases are those in which $|B| = |\bar{B}| = 2$, for which one finds

$$B = \{1, 3\},\ \bar{B} = \{2, 4\} : \mathcal{G}_0^B = \mathcal{G}_0^{\bar{B}} = \langle X_{01}Z_{01}Z_{02},\ X_{01}X_{02}\rangle; \tag{69}$$

$$B = \{1, 4\},\ \bar{B} = \{2, 3\} : \mathcal{G}_0^B = \mathcal{G}_0^{\bar{B}} = \langle X_{01}Z_{01},\ X_{02}Z_{02}\rangle; \tag{70}$$

$$B = \{1, 2\},\ \bar{B} = \{3, 4\} : \mathcal{G}_0^B = \mathcal{G}_0^{\bar{B}} = \langle X_{01}Z_{01},\ X_{02}Z_{02}\rangle. \tag{71}$$

In each case the generators commute and thus the subgroup $\mathcal{G}_0^B$ is Abelian. Hence the information is "classical," and the same type is present both in B and $\bar{B}$, not unlike the situation for the complete graph considered earlier. However, the three subgroups do not commute with each other, so the corresponding types of information are mutually incompatible, a situation similar to what we found for the bar graph.

For $D > 2$ it is again the case that all information is absent when $|B| = 1$ and completely present for $|B| \geqslant 3$. And (69) and (70) remain correct (with each generator of order D), and these subgroups are again Abelian. However, when $B = \{1, 2\}$ and $\bar{B} = \{3, 4\}$, (71) must be replaced with

$$\mathcal{G}_0^B = \langle Z_{01}X_{02}^2,\ Z_{02}\rangle, \quad \mathcal{G}_0^{\bar{B}} = \langle Z_{01},\ X_{01}^2 Z_{02}\rangle. \tag{72}$$

In each case the two generators do not commute with each other, so neither subgroup is Abelian. However, all elements of $\mathcal{G}_0^B$ commute with all elements of $\mathcal{G}_0^{\bar{B}}$. Also, the two subgroups are isomorphic (interchange subscripts 1 and 2).

For *odd* $D \geqslant 3$ one can use for $\mathcal{G}_0^B$ an alternative pair of generators

$$\mathcal{G}_0^B = \langle Z_{01}^m X_{02},\ Z_{02}\rangle, \quad m := (D+1)/2, \tag{73}$$

whose order is D and whose commutator is

$$\big(Z_{01}^m X_{02}\big)Z_{02} = \omega Z_{02}\big(Z_{01}^m X_{02}\big). \tag{74}$$

This means—see (8)—that $\mathcal{G}_0^B$, and thus also the (isomorphic) $\mathcal{G}_0^{\bar{B}}$, is isomorphic to the Pauli group of a single qudit. Since $\mathcal{G}_0^B$ and $\mathcal{G}_0^{\bar{B}}$ commute with each other, it is natural to think of the pair as associated with the tensor product of two qudits with the same D. That this is correct can be confirmed by explicitly constructing a "pre-encoding" circuit embodying the unitary

$$(\mathrm{F}_1 \otimes \mathrm{F}_2)^\dagger \mathrm{CP}_{12}^{-m}(\mathrm{F}_1 \otimes \mathrm{F}_2), \tag{75}$$

expressed in terms of the Fourier and CP gates defined in Sec. III B, that carries the Pauli groups on "pre-input" qudits 1 and 2 onto $\mathcal{G}_0^B$ and $\mathcal{G}_0^{\bar{B}}$, respectively.

Things become more complicated for *even* $D \geqslant 4$, where $\mathcal{G}_0^B$ (and also $\mathcal{G}_0^{\bar{B}}$) are no longer isomorphic to the Pauli group of a single qudit.

VII. CONCLUSION

We have shown that for additive graph codes with a set of n carrier qudits, each of the same dimension D, where D is any integer greater than 1, it is possible to give a precise characterization of the information from the coding space that is present in an arbitrary subset B of the carriers. This information corresponds to a subgroup $\mathcal{G}^B$ of a group $\mathcal{G}$, the information group of operators on the coding space, that spans the coding space and provides a useful representation of the information that it contains. We discuss how what we call a trivial code, essentially a tensor product of qudits of (possibly) different dimensions, can be encoded into the coding space in a manner which gives one a clear intuitive interpretation of $\mathcal{G}$. The subgroup $\mathcal{G}^B$ is then simply the subset of operators in $\mathcal{G}$ whose trace down to B is nonzero, and the traced-down operators when suitably normalized form a group $\mathcal{G}_B$ that is isomorphic to $\mathcal{G}^B$. The information present in those operators in $\mathcal{G}$ that are not in $\mathcal{G}^B$ disappears so far as the subsystem B is concerned, as their partial traces are zero. This is the central result of our paper and is illustrated by a number of simple examples in Sec. VI. We also provide in Appendix C a relatively simple algorithm for finding the elements of $\mathcal{G}^B$.

These results can be extended to arbitrary qudit stabilizer codes even if they are not graph codes, by employing appropriate stabilizer and information groups, as in Sec. IV. Here, however, the concept of a trivial code, and thus our perspective on the encoding step, may not apply. The extension of these ideas, assuming it is even possible, to more general codes, such as nonadditive graph codes, remains an open question.

As shown in Appendix D our formalism can be fitted within the general framework of invariant algebras as discussed in [16–19]. The overall conceptual framework we use is somewhat different from that found in these references in that we directly address the question of what information is present in the subsystem of interest, rather than asking whether there exists some recovery operation (the $\mathcal{R}$ in Appendix D) that will map an algebra of operators back onto its original space. Thus in our work the operator groups $\mathcal{G}^B$ on the coding space and $\mathcal{G}_B$ on the subsystem are isomorphic but not identical. Hence, even though there is, obviously, a close connection between our "group approach" and the "algebraic approach," the algebra of interest being generated from the group of operators, further relationships remain to be explored. The fact that the arguments in Appendix D are not altogether straightforward suggests that the use of groups in cases where this is possible may provide a useful supplement, both mathematically and intuitively, to other algebraic ideas. In particular the additional structure present in an additive graph code allows one to determine $\mathcal{G}^B$ in $O(n^\theta + K^2 n^2)$ (Appendix C) as against $O(K^6)$ for the algorithm presented in [19] for a preserved matrix algebra, where K is the dimension of the input and output Hilbert space.

ACKNOWLEDGMENTS

We thank Chang-You Lin for his contributions and Li Yu for useful discussions. The research described here received support from the National Science Foundation through Grants No. PHY-0456951 and No. PHY-0757251.

APPENDIX A: PROOF OF LEMMAS 1 AND 2

Proof of Lemma 1. The operators in $p\mathcal{R}$ are linearly independent when those in $\mathcal{R}$ are linearly independent, since p is unitary and thus invertible. This establishes (i). For (ii), consider the case where q is the identity I. As the collection

$\mathcal{R}$ is linearly independent, there is at most one $r \in \mathcal{R}$ such that pr is a multiple of the identity. If such an r exists, p is of the form $e^{i\phi}r^{-1}$, and since $\mathcal{R}$ is a group, $p\mathcal{R} = e^{i\phi}r^{-1}\mathcal{R} = e^{i\phi}\mathcal{R}$, we have situation ($\alpha$), with the collection $p\mathcal{R} \cup \mathcal{R}$ linearly dependent. Next assume the collection $p\mathcal{R} \cup \mathcal{R}$ is linearly dependent, which means there are complex numbers $\{a_r\}$ and $\{b_r\}$, not all zero, such that

$$\sum_{r\in\mathcal{R}} [a_r r + b_r pr] = 0. \tag{A1}$$

This is not possible if all the a_r are zero, since this would mean $p\sum_r b_r r = 0$, and thus $\sum_r b_r r = 0$, implying $b_r = 0$ for every r, since the $\mathcal{R}$ collection is by assumption linearly independent. Thus at least one a_r, say a_s is not zero. Multiply both sides of (A1) by s^{-1} on the right and take the trace:

$$a_s \mathrm{Tr}[I] + \sum_{r\in\mathcal{R}} b_r \mathrm{Tr}[prs^{-1}] = 0, \tag{A2}$$

implying there is at least one r for which $\mathrm{Tr}[prs^{-1}] \neq 0$. But then p is of the form $e^{i\phi}sr^{-1} = e^{i\phi}\bar{r}^{-1}$ for $\bar{r} = rs^{-1} \in \mathcal{R}$, so we are back to situation (α). Hence the alternative to (α) is (β): the operators in $p\mathcal{R} \cup \mathcal{R}$ are linearly independent. Finally, if q is not the identity I, simply apply the preceding argument with $\bar{p} = q^{-1}p$ in place of p.

Proof of Lemma 2. Statement (i) is a consequence of the fact that if an invertible operator is in $\mathcal{B}$, so is its inverse, and since $\mathcal{S}$ is a group, $g\mathcal{S}$ consists of the inverses of the elements in $g^{-1}\mathcal{S}$.

Statements (ii) and (iv) follow from a close examination of (55). Assume both sets on the left side are nonempty. If gs_1 and hs_2 are both in $\mathcal{B}$, so is their product $gs_1hs_2 = ghs_1s_2$, where we use the fact that g and h commute with every element of $\mathcal{S}$. If, on the other hand, $(gh\mathcal{S}) \cap \mathcal{B}$ and $(g\mathcal{S}) \cap \mathcal{B}$ are nonempty, any element, say ghs_1, in the former can be written using a specific element, say $g\bar{s}$, in the latter, as

$$ghs_1 = (g\bar{s})(hs_2), \tag{A3}$$

where $s_2 = s_1\bar{s}^{-1}$ is uniquely determined by this equation, and the fact that both ghs_1 and $g\bar{s}$ are (by assumption) in $\mathcal{B}$ means the same is true of hs_2. Thus not only can every element of $(gh\mathcal{S}) \cap \mathcal{B}$ be written as a product of elements of $(g\mathcal{S}) \cap \mathcal{B}$, but there is a one-to-one correspondence between $(gh\mathcal{S}) \cap \mathcal{B}$ and $(g\mathcal{S}) \cap \mathcal{B}$, which must therefore be of equal size. A similar argument shows that $(gh\mathcal{S}) \cap \mathcal{B}$ and $(h\mathcal{S}) \cap \mathcal{B}$ are of the same size. This establishes both (ii) and (iv).

As for (iii), use the fact that the cosets $g\mathcal{S}$ and $h\mathcal{S}$ are either identical or have no elements in common, so the same is true of their intersections with $\mathcal{B}$. If $g\mathcal{S}$ and $h\mathcal{S}$ have no elements in common, Lemma 1 with $\mathcal{R} = \mathcal{S}$ tells us that either $g\mathcal{S} = e^{i\phi}(h\mathcal{S})$ for some nonzero ϕ, in which case $\Sigma[(g\mathcal{S}) \cap \mathcal{B}] = e^{i\phi}\Sigma[(h\mathcal{S}) \cap \mathcal{B}]$ is distinct from $\Sigma[(h\mathcal{S}) \cap \mathcal{B}]$, or else the collection $(g\mathcal{S}) \cup (h\mathcal{S})$ is linearly independent, which means that its intersection with $\mathcal{B}$ shares this property and the operators $\Sigma[(g\mathcal{S}) \cap \mathcal{B}]$ and $\Sigma[(h\mathcal{S}) \cap \mathcal{B}]$ are linearly independent.

APPENDIX B: PROOF OF THEOREM 4

The proof of Theorem 4 makes use of the following:

Lemma 5. Let $\hat{g} = P\hat{g}P$ be an information operator in $\mathcal{G}$ with spectral decomposition

$$\hat{g} = \sum_{j=0}^{m-1} \lambda_j J_j, \tag{B1}$$

where the mutually orthogonal projectors J_j sum to P. Then each projector J_j can be written as a polynomial in $\hat{g}$ with $\hat{g}^0 = P$:

$$J_j = \sum_{k=0}^{m-1} \alpha_{jk}\hat{g}^k. \tag{B2}$$

Proof. The proof consists in noting that

$$\hat{g}^k = \sum_{j=0}^{m-1} \lambda_j^k J_j = \sum_{j=0}^{m-1} \beta_{kj} J_j \tag{B3}$$

is a linear equation in the J_j with $\beta_{kj} = \lambda_j^k$ an $m \times m$ Vandermonde matrix whose determinant is $\prod_{j>k}(\mu_j - \mu_k)$ (see p. 29 of [30]). As the μ_j are distinct the matrix β_{kj} has an inverse α_{jk}. ■

To prove (i) of Theorem 4, first assume that $\hat{g}$ is in $\mathcal{G}^B$. Since $\mathcal{G}^B$ is a group with identity P, this means that all powers of $\hat{g}$, including $\hat{g}^0 = P$, are also in $\mathcal{G}^B$. Consequently, the projectors entering the spectral decomposition (B1) of $\hat{g}$ satisfy

$$N^{-1}\mathrm{Tr}_{\bar{B}}[J_j]\mathrm{Tr}_{\bar{B}}[J_k] = \mathrm{Tr}_{\bar{B}}[J_j J_k] = \delta_{jk}\mathrm{Tr}_{\bar{B}}[J_j], \tag{B4}$$

with the first equality obtained by expanding J_j and J_k in powers of $\hat{g}$, (B2), and using (56) along with the linearity of the partial trace. This orthogonality of the partial traces of different projectors [see (3)] implies that the $\mathcal{J}(\hat{g})$ type of information is perfectly present in B. Conversely, if the $\mathcal{J}(\hat{g})$ type of information is perfectly present in B then the partial traces down to B of the different J_j, which cannot be zero, are mutually orthogonal and thus linearly independent. Therefore by (B1), $\mathrm{Tr}_{\bar{B}}[\hat{g}]$ cannot be zero, and $\hat{g}$ is in $\mathcal{G}^B$.

The prove (ii) note that $\hat{g}^k$ absent from $\mathcal{G}^B$ for $1 \leqslant k < D$ means that $\mathrm{Tr}_{\bar{B}}[\hat{g}^k] = 0$ for these values of k, and thus by taking the partial trace of both sides of (B2) and using (57),

$$\mathrm{Tr}_{\bar{B}}[J_j] = N\alpha_{j0}P_B. \tag{B5}$$

Since these partial traces are identical up to a multiplicative constant there is no information of the $\mathcal{J}(\hat{g})$ type in B. For the converse, if there is no $\mathcal{J}(\hat{g})$ information in B then there is also no $\mathcal{J}(\hat{g}^2)$, $\mathcal{J}(\hat{g}^3)$, etc. information in B, since the projectors which arise in the spectral decomposition of $\hat{g}^k$ are already in the spectral decomposition of $\hat{g}$ [see (B3)]. Consequently, by (i), these $\hat{g}^k$ must be absent from $\mathcal{G}^B$.

To prove (iii), note that if all information is perfectly present in B this means that for every $\hat{g} \in \mathcal{G}$ the $\mathcal{J}(\hat{g})$ information is present in B, and therefore, by (i), $\hat{g} \in \mathcal{G}^B$, so $\mathcal{G} = \mathcal{G}^B$. For the converse, let Q_1 and Q_2 be two orthogonal but otherwise arbitrary projection operators on subspaces of the coding space $\mathcal{H}_C$. Because the elements of the information group $\mathcal{G}$ form a basis for the set of linear operators on $\mathcal{H}_C$ (see comments at the end of Sec. IV C), Q_1 and Q_2 can both be written as sums of elements $\hat{g}$ in $\mathcal{G}$, and the same argument that was employed in (B4) shows that the orthogonality of Q_1 and Q_2 implies the orthogonality of $\mathrm{Tr}_{\bar{B}}[Q_1]$ and $\mathrm{Tr}_{\bar{B}}[Q_2]$.

To prove (iv), note that if $\mathcal{G}^B$ consists entirely of scalar multiples of P, the partial trace down to B of any projector Q on a subspace of $\mathcal{H}_C$, since it can be written as a linear combination of the partial traces of the $\hat{g}$ in $\mathcal{G}$, most of which vanish, will be some multiple of P_B, and thus all information is absent from B. Conversely, if $\mathcal{G}^B$ contains a $\hat{g}$ which is not proportional to P the corresponding $\mathcal{J}(\hat{g})$ type of information will be present in B by (i), so it is not true that all information is absent from B, which is a contradiction.

APPENDIX C: ALGORITHM FOR FINDING $\mathcal{G}^B$

Here we present an algorithm for determining the subset information group $\mathcal{G}^B$ by finding the elements $\hat{g}$ of $\mathcal{G}$ whose partial trace down to B is nonzero. If two or more elements differ only by a phase it is obviously only necessary to check one of them. For what follows it is helpful to adopt the abbreviation

$$E^{(\mathbf{x}|\mathbf{z})} := X^{\mathbf{x}} Z^{\mathbf{z}}, \tag{C1}$$

with $(\mathbf{x}|\mathbf{z})$ an n-tuple row vector pair, and thus a $2n$-tuple of integers between 0 and $D-1$. Arithmetic operations in the following analysis are assumed to be mod D.

First consider the trivial code on the trivial graph (Sec. IV B), with information group $\mathcal{G}_0^B$ consisting of elements of the form $\hat{g}_0 = g_0 P_0$ [see (48)], with $g_0 = E^{(\mathbf{x}_0|\mathbf{z}_0)}$ some element of $\mathcal{W}_0 = \langle \mathcal{S}_0^G, \mathcal{C}_0 \rangle$, and

$$P_0 = |\mathcal{S}_0|^{-1} \sum_{\mathbf{x}\in\mathcal{X}_0} X^{\mathbf{x}}, \tag{C2}$$

where $\mathcal{X}_0$ denotes the collection of n-tuples that enter the stabilizer $\mathcal{S}_0$, (37). By choosing $\mathbf{x}_0$ and $\mathbf{z}_0$ to be of the form

$$\begin{aligned} \mathbf{x}_0 &= (\xi_1, \xi_2, \ldots \xi_k, 0, 0, \ldots 0), \\ \mathbf{z}_0 &= (\zeta_1 m_1, \zeta_2 m_2, \ldots \zeta_k m_k, 0, 0, \ldots 0), \end{aligned} \tag{C3}$$

using integers in the range

$$0 \leqslant \xi_j \leqslant (d_j - 1), \quad 0 \leqslant \zeta_j \leqslant (d_j - 1), \tag{C4}$$

we obtain a single representative $g_0 = E^{(\mathbf{x}_0|\mathbf{z}_0)}$ for each coset $g_0\mathcal{S}_0$ in $\mathcal{W}/\mathcal{S}_0$. The corresponding information operator, which depends only on the coset, is

$$\hat{g}_0 = E^{(\mathbf{x}_0|\mathbf{z}_0)} P_0 = |\mathcal{S}_0|^{-1} \sum_{\mathbf{x}\in\mathcal{X}_0} \omega^{-\mathbf{z}_0\mathbf{x}} E^{(\mathbf{x}+\mathbf{x}_0|\mathbf{z}_0)}, \tag{C5}$$

where the addition of $\mathbf{x}$ and $\mathbf{x}_0$ is component-wise mod D, and $\mathbf{z}_0\mathbf{x}$ denotes the scalar product of $\mathbf{z}_0$ and $\mathbf{x}$ mod D (multiply corresponding components and taking the sum mod D).

Elements of the information group $\mathcal{G}^B$ of the nontrivial code of interest to us are then of the form

$$\begin{aligned} \hat{g} &= (UW)\hat{g}_0(UW)^\dagger \\ &= |\mathcal{S}_0|^{-1} \sum_{\mathbf{x}\in\mathcal{X}_0} \omega^{\nu(\mathbf{x},\mathbf{x}_0,\mathbf{z})-\mathbf{z}_0\mathbf{x}} E^{(\mathbf{x}+\mathbf{x}_0|\mathbf{z}_0)Q}, \end{aligned} \tag{C6}$$

where we use the fact that because the conjugating operator UW, (36), is a Clifford operator there is a $2n \times 2n$ matrix Q over $\mathbb{Z}_D^{2n}$, representing a symplectic automorphism [23], such that

$$(UW)E^{(\mathbf{x}|\mathbf{z})}(UW)^\dagger = \omega^{\nu(\mathbf{x},\mathbf{z})} E^{(\mathbf{x}|\mathbf{z})Q}, \tag{C7}$$

with $(\mathbf{x}|\mathbf{z})Q$ the $2n$-tuple, interpreted as an n-tuple pair, obtained by multiplying $(\mathbf{x}|\mathbf{z})$ on the right by Q, and $\nu(\mathbf{x},\mathbf{z})$ an integer whose value does not concern us. The explicit form of Q can be worked out by means of the encoding procedure presented in Sec. IV B, using Tables I and II.

The operators appearing in the sum on the right side of (C6) are linearly independent Pauli products, since Q is nonsingular. The trace down to B of such a product is nonzero if and only if its base is in B, and when nonzero the result after the trace is essentially the same operator: see (53) and the associated discussion. Consequently $g_B = N^{-1}\mathrm{Tr}_{\bar{B}}[\hat{g}]$ is nonzero if and only if the trace down to B of at least one operator on the right side of (C6) is nonzero. A useful test takes the form

$$\mathrm{Tr}_{\bar{B}}[E^{(\mathbf{x}|\mathbf{z})}] \neq 0 \Longleftrightarrow (\mathbf{x}|\mathbf{z})J = \mathbf{0}, \tag{C8}$$

where $\mathbf{0}$ is the zero row vector, and J is a diagonal $2n \times 2n$ matrix with 1 at the diagonal positions j and $j+n$ whenever qudit j belongs to $\bar{B}$, and 0 elsewhere. Therefore the $\hat{g}$ associated with $\mathbf{x}_0$ and $\mathbf{z}_0$ through (C5) and (C6) is a member of $\mathcal{G}^B$ if and only if there is at least one $\mathbf{x} \in \mathcal{X}_0$ such that

$$(\mathbf{x}+\mathbf{x}_0|\mathbf{z}_0)QJ = \mathbf{0} \quad \text{or} \quad (\mathbf{x}|\mathbf{0})QJ = -(\mathbf{x}_0|\mathbf{z}_0)QJ. \tag{C9}$$

The $\mathbf{x}$ that belong to $\mathcal{X}_0$ are characterized by the equation

$$\mathbf{x}M = \mathbf{0}, \tag{C10}$$

where M is an $n \times k$ matrix that is everywhere 0 except for $M_{jj} = m_j$ for $1 \leqslant j \leqslant k$, using the m_j that appear in (28). Consequently, instead of asking whether (C9) has a solution $\mathbf{x}$ belonging to $\mathcal{X}_0$ one can just as well ask if there is any solution to the pair (C9) and (C10), or equivalently to the equation

$$\mathbf{x}T = \mathbf{u}_0, \tag{C11}$$

where T is an $n \times (2n+k)$ matrix whose first $2n$ columns consist of the top half of the matrix QJ (upper n elements of each column), and whose last k columns are the matrix M in (C10), while $\mathbf{u}_0$ is a row vector whose first $2n$ elements are $-(\mathbf{x}_0|\mathbf{z}_0)QJ$ and last k elements are 0. Deciding if (C11) has a solution $\mathbf{x}$ becomes straightforward once one has transformed T to Smith normal form, including determining the associated invertible matrices [see (32)]. As this needs to be done just once for a given additive code and a given subset B, the complexity of the algorithm for finding $\mathcal{G}^B$ is $O(n^\theta)$ for finding the Smith form plus $O(n^2K^2)$ for testing the K^2 elements of $\mathcal{G}$ once the Smith form is available. By using the group property of $\mathcal{G}^B$ one can construct a faster algorithm, but that is beyond the scope of this paper.

APPENDIX D: CORRECTABLE $*$-ALGEBRA

The counterpart in [17] of our notion of information perfectly present at the output of a quantum channel (see Sec. II) is that of a *correctable $*$-algebra* $\mathcal{A}$ of operators acting on a Hilbert space. The $*$ (sometimes denoted C$*$) means that $\mathcal{A}$, as well as being an algebra of operators in the usual sense, contains $a^\dagger$ whenever it contains a. Let the channel superoperator $\mathcal{E}$ be represented by Kraus operators,

$$\mathcal{E}(\rho) = \sum_j E_j \rho E_j^\dagger, \tag{D1}$$

satisfying the usual closure condition $\sum_j E_j^\dagger E_j = I$, and let P be a projector onto some subspace $P\mathcal{H}$ of the Hilbert space $\mathcal{H}$. Then a $*$-algebra $\mathcal{A}$ is defined in [17] to be *correctable for $\mathcal{E}$ on states in $P\mathcal{H}$* provided $a = PaP$ for every a in $\mathcal{A}$, and there exists a superoperator $\mathcal{R}$ (the recovery operation in an error correction scheme) whose domain is the range of $\mathcal{E}$, whose range is $\mathcal{L}(\mathcal{H})$, and such that

$$P[(\mathcal{R}\circ\mathcal{E})^\dagger(a)]P = a = PaP \tag{D2}$$

for all $a \in \mathcal{A}$. Here the dagger denotes the adjoint of the superoperator in the sense that

$$\mathrm{Tr}\{b[(\mathcal{R}\circ\mathcal{E})(c)]\} = \mathrm{Tr}\{[(\mathcal{R}\circ\mathcal{E})^\dagger(b)]c\} \tag{D3}$$

for any b and c in $\mathcal{L}(\mathcal{H})$. In [17] (see Theorem 9 and Corollary 10), it is shown that any correctable algebra in this sense is a subalgebra of (what we call) a *maximal* correctable algebra

$$\mathcal{A}_M = \{a \in \mathcal{L}(P\mathcal{H}) : [a, PE_i^\dagger E_j P] = 0 \quad \forall\, i, j\}. \tag{D4}$$

We can apply this to our setting described in Secs. IV and V where P is the projector on the coding space $\mathcal{H}_C$ and $\mathcal{E}_B$ is the superoperator for the partial trace down to the subset B of carriers,

$$\mathcal{E}_B(\rho) = \mathrm{Tr}_{\bar{B}}[\rho] = \sum_j E_j \rho E_j^\dagger \quad \text{for} \quad \rho \in \mathcal{L}(\mathcal{H}) \tag{D5}$$

with Kraus operators

$$E_j := I_B \otimes \langle j|_{\bar{B}}\,, \tag{D6}$$

where $|j\rangle_{\bar{B}}$ is any orthonormal basis of $\mathcal{H}_{\bar{B}}$, so

$$E_i^\dagger E_j = I_B \otimes |i\rangle\langle j|_{\bar{B}}\,. \tag{D7}$$

We shall now show that the collection of operators in $\mathcal{G}^B$ (defined in Theorem 3) spans a $*$-algebra which is correctable for $\mathcal{E}_B$ on states in $P\mathcal{H} = \mathcal{H}_C$ and is the maximal algebra of this kind, i.e. $\mathrm{span}(\mathcal{G}^B) = \mathcal{A}_M$. First note that $\mathrm{span}(\mathcal{G}^B)$ is indeed a $*$-algebra: every $\hat{g} \in \mathcal{G}$ is a unitary operator and $\mathcal{G}$ contains the adjoint of each of its elements; replacing g with $g^\dagger$ in (48) yields $\hat{g}^\dagger$. Of course $\mathrm{Tr}_{\bar{B}}[\hat{g}] = 0$ if and only if $\mathrm{Tr}_{\bar{B}}[\hat{g}^\dagger] = 0$ and, in addition, $a = PaP$ for $a \in \mathrm{span}(\mathcal{G}^B)$ because $\hat{g} = P\hat{g}P$, (48).

By definition $\mathrm{Tr}_{\bar{B}}[\hat{g}] \neq 0$ for $\hat{g} \in \mathcal{G}^B$, and this means that the partial trace down to B of at least one element in the corresponding coset $g\mathcal{S}$ [see (48)] must be nonzero. Let h be such an element; since it is a Pauli product it must be of the form $h = h_B \otimes I_{\bar{B}}$. As a consequence,

$$\begin{aligned}[\hat{g}, PE_i^\dagger E_j P] &= [\hat{h}, PE_i^\dagger E_j P] = P[h, E_i^\dagger E_j]P \\ &= P[h_B \otimes I_{\bar{B}}, I_B \otimes |i\rangle\langle j|_{\bar{B}}]P = 0,\end{aligned} \tag{D8}$$

where the successive steps are justified as follows. Since $\hat{g}$ depends only on the coset $g\mathcal{S}$ and h belongs to this coset, $h\mathcal{S} = g\mathcal{S}$ and $\hat{h} = Ph = hP = \hat{g}$. This means we can move the projector P outside the commutator bracket, and once outside it is obvious that the latter vanishes for every i and j. Thus any $\hat{g}$ in $\mathcal{G}^B$ belongs to the maximal $\mathcal{A}_M$ defined in (D4), as do all linear combinations of the elements in $\mathcal{G}^B$.

To show that $\mathcal{A}_M$ is actually spanned by $\mathcal{G}^B$ we note that any a belonging to $\mathcal{A}_M$ can be written as

$$a = b + c, \tag{D9}$$

where b is a linear combination of elements of $\mathcal{G}^B$ and c of elements of $\mathcal{G}$ that do not belong to $\mathcal{G}^B$, so $\mathrm{Tr}_{\bar{B}}[c] = \mathrm{Tr}_{\bar{B}}[c^\dagger] = 0$. Thus it is the case that

$$P(\mathcal{R}\circ\mathcal{E}_B)^\dagger(b)P = b, \quad P(\mathcal{R}\circ\mathcal{E}_B)^\dagger(c)P = c, \tag{D10}$$

where the first follows [see (D2)] from the previous argument showing that the span of $\mathcal{G}^B$ is a subalgebra of $\mathcal{A}_M$, and the second from linearity and the assumption that a belongs to $\mathcal{A}_M$. Multiply the second equation by $c^\dagger$ and take the trace:

$$\begin{aligned}\mathrm{Tr}[c^\dagger c] &= \mathrm{Tr}\{c^\dagger P[(\mathcal{R}\circ\mathcal{E}_B)^\dagger(c)]P\} \\ &= \mathrm{Tr}\{[\mathcal{R}\circ\mathcal{E}_B(c^\dagger)]c\} = 0,\end{aligned} \tag{D11}$$

where we used the fact that $Pc^\dagger P = c^\dagger$, and $\mathcal{E}_B(c^\dagger) = \mathrm{Tr}_{\bar{B}}[c^\dagger] = 0$. Thus $c = 0$ and any element of $\mathcal{A}_M$ is a linear combination of the operators in $\mathcal{G}^B$.

In conclusion, we have shown for any additive graph code C and any subset of carrier qudits B, the $*$-algebra spanned by operators in $\mathcal{G}^B$ is exactly the maximal correctable algebra $\mathcal{A}_M$ defined in (D4). In Appendix C we outline an algorithm that enumerates the elements in $\mathcal{G}^B$ for any $\mathcal{H}_C$ and $\mathcal{E}_B$, which in light of the result above is an operator basis of $\mathcal{A}_M$.

[1] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
[2] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[3] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[4] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Mathematical Library, Amsterdam, 1977).
[6] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[7] R. B. Griffiths, Phys. Rev. A **71**, 042337 (2005).
[8] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A **78**, 042303 (2008).
[9] D. Schlingemann, e-print arXiv:quant-ph/0111080.
[10] M. Grassl, A. Klappenecker, and M. Roetteler, in *Proceedings of the 2002 IEEE International Symposium on Information Theory* (IEEE, New York, 2002).
[11] D. Gottesman, Chaos Solitons Fractals **10**, 1749 (1999), e-print arXiv:quant-ph/9802007.
[12] E. M. Rains, IEEE Trans. Inf. Theory **45**, 1827 (1999).
[13] D. Schlingemann and R. F. Werner, Phys. Rev. A **65**, 012308 (2001).
[14] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu, and C. H. Oh, Phys. Rev. A **78**, 012306 (2008).
[15] L. Ioffe and M. Mézard, Phys. Rev. A **75**, 032345 (2007).
[16] C. Bény, A. Kempf, and D. W. Kribs, Phys. Rev. Lett. **98**, 100502 (2007).

[17] C. Bény, A. Kempf, and D. W. Kribs, Phys. Rev. A **76**, 042303 (2007).
[18] C. Bény, e-print arXiv:0907.4207 [quant-ph].
[19] R. Blume-Kohout, H. K. Ng, D. Poulin, and L. Viola, Phys. Rev. Lett. **100**, 030501 (2008).
[20] R. B. Griffiths, Phys. Rev. A **76**, 062320 (2007).
[21] R. B. Griffiths, Phys. Rev. A **54**, 2759 (1996).
[22] R. B. Griffiths, *Consistent Quantum Theory* (Cambridge University Press, Cambridge, England, 2002).
[23] E. Hostens, J. Dehaene, and B. DeMoor, Phys. Rev. A **71**, 042315 (2005).
[24] M. Newman, *Integral Matrices* (Academic Press, New York, 1972).
[25] A. Storjohann, *ISSAC '96: Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation* (ACM Press, New York, 1996), p. 267.
[26] D. Coppersmith and S. Winograd, in *STOC '87: Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing* (ACM, New York, 1987), p. 1.
[27] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 5th ed. (Cambridge University Press, Cambridge, England, 2000).
[28] M. Grassl, T. Beth, and T. Pellizzari, Phys. Rev. A **56**, 33 (1997).
[29] S. Yu, Q. Chen, and C. Oh, e-print arXiv:0709.1780 [quant-ph].
[30] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, England, 1999).